Configurer Windows Server pour transférer les requêtes DNS vers Umbrella

Table des matières

Introduction

Aperçu

Configuration Steps

Remarques sur les meilleures pratiques

Introduction

Ce document décrit comment configurer Windows Server pour transférer des requêtes DNS à Umbrella pour une protection et une journalisation client améliorées.

Aperçu

Windows Server peut protéger les clients utilisant une identité réseau en agissant comme redirecteur DNS. Les contrôleurs de domaine ou tout autre serveur ayant le rôle DNS peuvent envoyer des DNS à Umbrella à partir d'un réseau enregistré.

Configuration Steps

1. Ouvrez le Gestionnaire DNS (dnsmgmt.msc).
2. Cliquez avec le bouton droit sur le nom du serveur dans l'arborescence et sélectionnez Propriétés.
3. Sélectionnez l'onglet Redirecteurs.
4. Cliquez sur Edit... et entrez les adresses IP du serveur DNS Umbrella.
5. Cliquez sur OK dans la fenêtre Modifier les redirecteurs. Les entrées s'affichent dans la liste des redirecteurs.
6. Décochez la case Utiliser les indications de racine si aucun redirecteur n'est disponible.



Remarques sur les meilleures pratiques

- Assurez-vous que l'option Utiliser les indications de racine si aucun redirecteur n'est disponible reste désactivée. Si cette case est cochée, la protection et la journalisation du parapluie deviennent incohérentes. Par exemple, si un domaine échoue à la validation DNSSEC ou est soumis à un événement de limitation DDoS, le serveur DNS Windows peut considérer Umbrella comme ne répondant pas et tenter une récursivité directe en utilisant des indications de racine, en contournant Umbrella.

- Utilisez uniquement Umbrella comme transitaires. Ne configurez aucun programme de résolution tiers. Umbrella peut uniquement enregistrer et protéger les requêtes DNS qu'il reçoit.

- Pour la redondance, configurez les quatre adresses IP Umbrella anycast en tant que redirecteurs, comme indiqué dans la capture d'écran précédente.

- Si vous utilisez des sites Umbrella et des appliances virtuelles, pointez vers une appliance virtuelle locale en tant que redirecteur au lieu d'adresses anycast Umbrella.

    - Éviter les boucles de requête : Si une appliance virtuelle répertorie votre serveur comme l'un de ses serveurs DNS locaux, n'ajoutez pas cette appliance virtuelle en tant que redirecteur.
    - Une appliance virtuelle ne voit que l'adresse IP du serveur DNS, et non les adresses des clients individuels qu'elle dessert.
    - Si vous utilisez l'intégration Active Directory avec l'appliance virtuelle, ajoutez l'adresse IP du serveur DNS Windows comme exception. Accédez à Déploiements > Sites et Active Directory > Exceptions de compte de service dans le tableau de bord Umbrella et ajoutez l'adresse IP du serveur DNS. Cela empêche l'attribution incorrecte des identités d'utilisateur au trafic du serveur.

- N'ajoutez pas de serveurs Umbrella à l'onglet Root Hints. Les serveurs DNS parapluie sont des résolveurs récursifs et ne servent pas de racines pour les recherches itératives. Les ajouter en tant qu'indications de racine entraîne un comportement indésirable et contourne la protection et la journalisation Umbrella.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.